International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

# Secure File Storage on Cloud using Cryptography

**Authors:** Paras Kamble Ganesh Patil Snehal Maliya Aniket Nimbalkar

Computer Department of Engineering,
JSPM BSIOTR, WAGHOLI,
PUNE, INDIA.

***Abstract*- We can share anything by just clicking a button on our computers. Due to this digitalization for sharing data with the world, the need for security is very important nowadays while transferring any data on the internet. To overcome data leaks and secure sensitive data cryptography is used. The word Cryptography itself defines its meaning which is "crypt" meaning "hidden and "graphy" stands for "writing". Cryptography plays an important role in sharing sensitive data using different algorithms for encrypting and decrypting the data while transferring data on the internet such as for sending important bank documents, military-related data, information of any company, or files related to an organization, or even a medical report. Cloud computing is beneficial in terms of low cost and accessibility of data. In this paper, we have reviewed a system that has a hybrid algorithm mechanism to store and secure the data in the cloud and transfer it, so even if there's any security breach the hacker won't be able to find out which algorithm was used to encrypt the data. In this system 3 different algorithms are used which are AES, 3DES, RC6 to encrypt and decrypt the data. Hence to securely share the information by splitting data into several chunks by applying different algorithms for encryption and storing parts of it on the cloud, and again applying decryption at the receiver's side to receive the data which was shared cryptography is used. This type of technology ensures that there is stronger data security and by using cloud computing in our system there is data availability.**

***Keywords: Security, Cryptography, AES, 3DES, RC6, Cloud-computing.***

## I. INTRODUCTION

At the beginning of the digital era in the 1950s even writing the data and storing it on a computer was considered a big thing. It was hard to store the data because many companies and organizations were trying to digitalize and were storing data on the computer; earlier a big wall-sized hard drive was used to store just a 5MB (megabyte) of data. Due to this era, the amount of data kept increasing and increasing which lead to the development of data storage devices such as hard-disk, hard-drives, compact-disk, pen-drives, computers with big storage capacity but this lead to increasing more physical storage techniques which lead to more problems such as storing the database on your computer working on it then again storing the updated data on the system's data was more insecure because anyone can steal your devices such as your pen-drive, CD's, hard-drives and also the amount of physical storage kept increasing hence to overcome this big-data issue and data security cloud storage, cloud computing was introduced in late 1990s.

Cloud computing is the concept that is used for handling big amount of data or for sharing sensitive data. It's the best way to use and compute data from anywhere in the world irrespective of your system specifications at the present timeline we can use a big amount of data anytime and anywhere with cloud computing. Every one or the other web application we use it uses cloud computing, for example, Google, Gmail, YouTube, even online games the only thing we should have is high-speed internet and a system to run that internet and we are good to go. But no matter what system we use whether it is online (cloud computing) or offline (desktop computers systems) or both even to run the cloud computing we have to use servers that are stored somewhere secured and anonymous.

The hackers try to steal your data no matter what or where we store so it's our responsibility to secure our data and keep it safe and share it safely. But when we have to share sensitive data where data security is the first priority such as military data, government-related information, medical reports we have to share the data in such a way that even if the data gets stolen one can't get to know what it was. Therefore, cryptography is used to share the data for encryption and decryption. Cryptography is basically just different types of algorithms to encrypt and decrypt it again some examples of algorithms such as MD5, SHA1, SHA256, Blowfish, AES, DES, 3DES, RC5, RC6, etc. are usually used. As the technology increases these algorithms got developed day by day. In this paper, we have reviewed a system that uses a hybrid algorithm that has AES, 3DES, and RC6.

## II. REQUIREMENTS

- Hardware Requirements:
  - Pentium Processor Core 2 Duo or Higher
  - Hard Disk: 250 GB (min)
  - RAM: 1GB or higher.
  - Processor speed: 3.2 GHz or faster processor.
- Software Requirements:
  - Python installed on your system
  - Any Python IDE (PyCharm, Spyder, etc.)
  - Stable internet
  - 7zip to extract .txt file from an image

## III. SYSTEM DESIGN

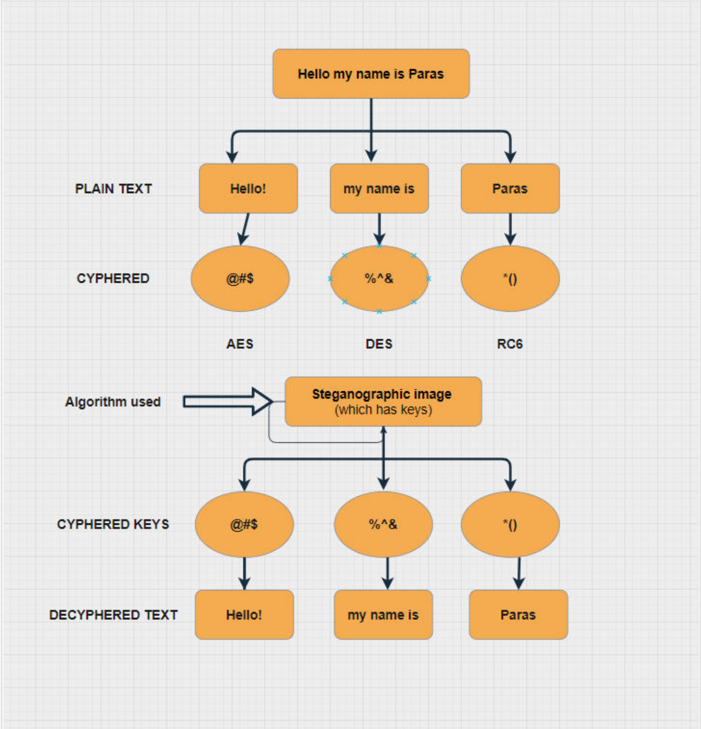

Fig (1) Structure diagram of the system

This is the structure diagram of the system which we have used. The system is designed to store the sensitive data using hybrid cryptography algorithm & then that file is hidden and shared using image steganography. In this system first plain text is stored at the sender's side. Then that message is divided into three parts. These three parts are given to the algorithm AES, DES and RC6 to cypher the given data and stored in a .png extension file anonymously; this image file is shared on the cloud and it's deciphered using the three algorithms at the receiver's side. The flowchart of the system is as follows:

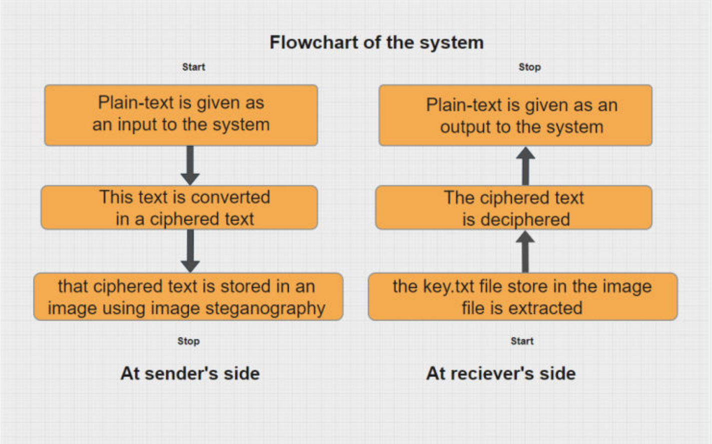
Flowchart of the system
Start
Plain-text is given as an input to the system
This text is converted in a ciphered text
that ciphered text is stored in an image using image steganography
Stop
At sender's side
Stop
Plain-text is given as an output to the system
The ciphered text is deciphered
the key.txt file store in the image file is extracted
Start
At reciever's side

Fig (2) Flow-chart diagram of the system

## IV. LEARNING METHODOLOGY

### (i) AES Algorithm:

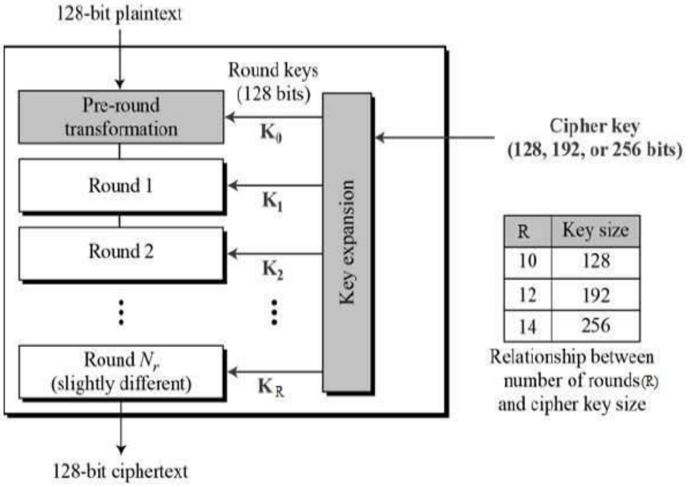

Fig (3) AES Algorithm diagram

**Asymmetric Encryption Standard** (**AES**)Algorithm is an algorithm which was developed by Vincent Rijmen and Joan Daemen at the National Institute of standards and technology (NIST) in October 2000. This algorithm is basically a subset of the Rijndael block cipher published in 1998. This algorithm converts 128bits block-sized data into 128 bit cyphered data with key sizes that differ from 128bits, 192bits, 256bits. This algorithm is a symmetrical-key algorithm i.e., same key used for encryption as well as for decryption. In this paper, we have reviewed a system that uses the AES algorithm which is one of the hybrid algorithms of the system. This algorithm follows certain steps in one round and these rounds are repeated no. of times depending on the key size i.e., 10 rounds for key-size of 128bits 12 rounds for key-size of 192bits and 14 rounds for key-size of 256bits. The working of this algorithm is as follows:

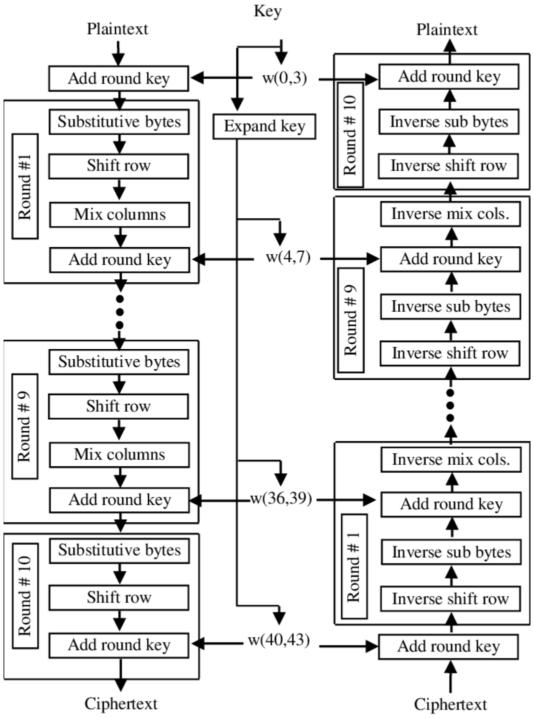

Fig (4) AES Structure diagram

(1) XOR - The plaintext is stored in a 128bit sized block data in matrix format and XOR operation is performed on this block (These blocks are further sub-divided into sub-blocks. For better understanding we can imagine that these sub-blocks can be represented in a Matrix representation which has rows and columns.)

(2) Sub Bytes - The blocks are substituted to make the algorithm as complex as possible and hard to decipher.

(3) Shift Rows & Mix rows - The rows are shifted at the same time the columns are mixed in the matrix

(4) Add Key - And then at the end, our key is added to this cyphered text.

These steps of the round are repeated depending on the key size as mentioned earlier This is the working of one of the algorithms used in our reviewed system. AES algorithm is just the first algorithm of our hybrid algorithm system. In this system the data is divided into three parts and those 3 parts are encrypted and stored hidden in an image format file using image steganography on cloud for increasing higher security of our data.

(ii) DES Algorithm:

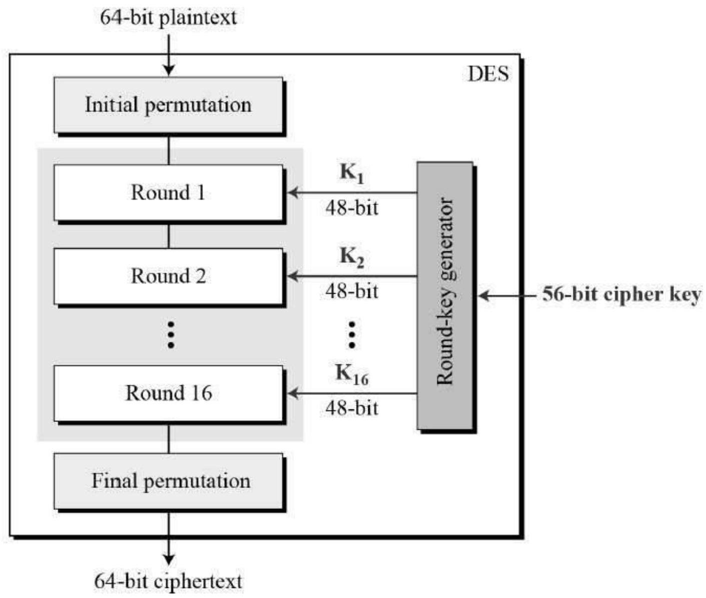

Fig (5) DES Algorithm diagram

Data Encryption Standard (DES) Algorithm The data encryption standard is a symmetric key block cipher published by the national institute of standards and technology (NIST) DES is an implementation of Feistel Cipher. It uses a 16 round Feistel Structure. The block size is 64 bits. though the key length is 64-bit, DES has an effective key length of 56 bits since 8 of the 64 bits of the key are not used by the encryption algorithm. The key is stored or transmitted as 8 bytes, each with odd parity. Before the main rounds, the block is divided into two 32-bit halves and processed alternately; this crisscrossing is known as the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar processes—the only difference is that the subkeys are applied in the reverse order when decrypting.

Initial and Final Permutation. The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES.

Round Function: The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

Expansion Permutation Box - Since the right input is 32-bit and the round key is a 48-bit, we

first, need to expand the right input to 48 bits.

XOR (Whitener) - After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

Substitution Boxes - The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with 6-bit input and a 4-bit output.

Key generation - The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The logic for Parity drop, shifting, and Compression P-box.

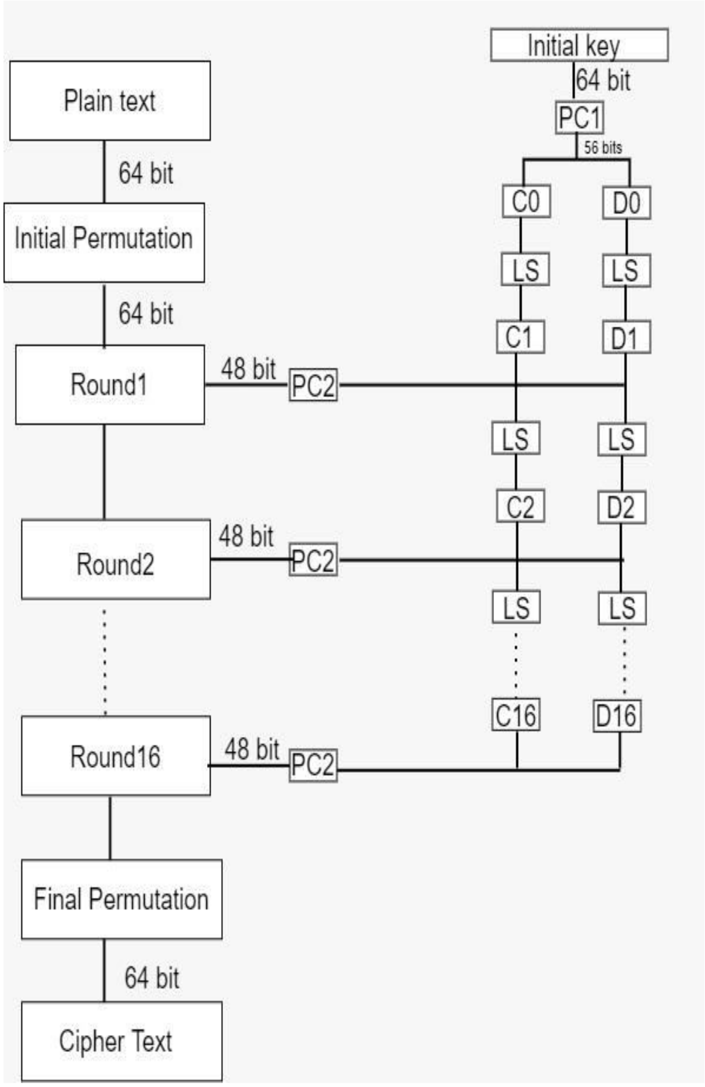

Fig (6) DES Structure diagram

(iii) RC6 Algorithm:

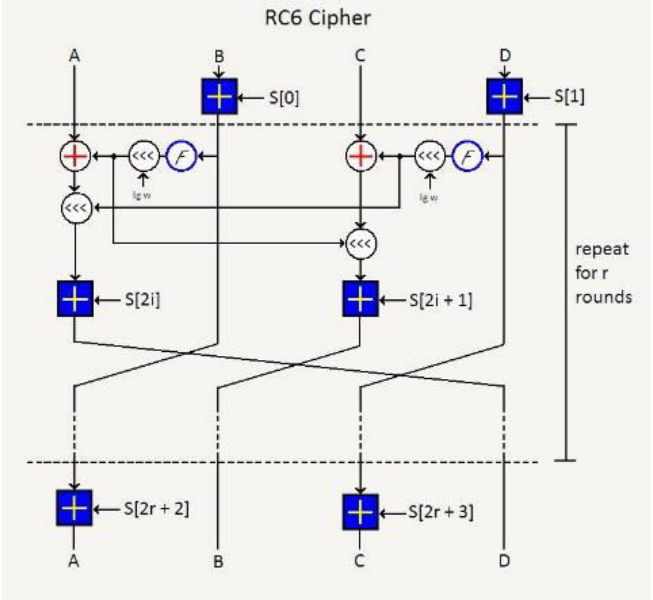

Fig (7) DES Structure diagram

RC6 (Rivest Cipher 6) is a symmetric key block cipher. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney, Yiqun Lisa Yin to meet the requirements of the AES Competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits up to 2040 bits.it may be parameterized to support a wide variety of word lengths, key sizes, and a number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes, although RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits.

## V. CONCLUSION

The project we have reviewed in this paper has a Hybrid mechanism that has 3 algorithms AES, DES, RC6 in it. Due to this strong algorithm mechanism the hacker won’t be able to guess the algorithm which we have used for encryption and our cipher text/key.txt file will be secure even if it’s caught. Our message is secure, scalable, and available to everyone. Only the users who know that we have hidden keys.txt file inside our image file will extract the data from it and decrypt that message and get the information file which we will share on the cloud. So even if our data gets stolen the hacker won't be able the know what are we sharing in those images with the help of image steganography.

## REFERENCES

[1] Selvanayagam, J., Singh, A., Michael, J., & Jeswani, J. (2018). Secure file storage on cloud using cryptography. International Research Journal of Engineering and Technology, 5(2), 2044–2047.

[2] Poduval, A., & others (2019). Secure File Storage on Cloud using Hybrid Cryptography. International Journal of Computer Science and Engineering, 7.

[3] Kanatt, S., Jadhav, A., & Talwar, P. Review of Secure File Storage on Cloud using Hybrid Cryptography.

[4] Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012, October). Secure storage and access of data in cloud computing. In 2012 International Conference on ICT Convergence (ICTC) (pp. 336-339). IEEE.J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

[5] Mahalle, V. S., & Shahade, A. K. (2014, October). Enhancing the data security in cloud by implementing hybrid (RSA & AES) encryption algorithm. In 2014 International Conference on Power, Automation and Communication (INPAC) (pp. 146-149). IEEE.

[6] Uddin, M. P., Saha, M., Ferdousi, S. J., Afjal, M. I., & Marjan, M. A. (2014, October). Developing an efficient solution to information hiding through text steganography along with cryptography. In 2014 9th International Forum on Strategic Technology (IFOST) (pp. 14-17). IEEE.

## AUTHORS

**First Author** – Paras Sanjay Kamble, pursuing BE(Comp), JSPM BSIOTR (Wagholi) Pune,

**Second Author** – Snehal Maliya, pursuing BE(Comp), JSPM BSIOTR (Wagholi) Pune.

**Third Author** – Ganesh Kishore Patil, pursuing BE(Comp), JSPM BSIOTR (Wagholi) Pune.